

TSE Services



Touchstone Energy®

## **SEIM – Security Event Information Management**

August 14, 2009

11:15 AM

*2009 Technology Conference*

*Myrtle Beach, South Carolina*



# Island EMC Everyone Needs Security

## COMPU-TOON



**GET READY...AN ELECTRIC EEL IS COMING  
THIS WAY!**



# Agenda

1. Introduction
2. Who we are
3. SEIM Definition
4. Functions
5. Requirements
6. Business Drivers
7. Not enough time
8. How do you show compliance
9. Vendors
10. Questions

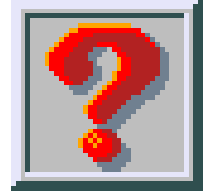


# Speaker



- Robert Thompson– Senior Systems Engineer
- TSE Services, LLC - Raleigh, NC
- Responsibility – Engineering design and daily operation of Telecommunication and Wide Area Networking for the North Carolina Electric Membership Corporation (NCEMC)
- NCEMC – G&T owned by Electric Membership Cooperatives (EMC) within the state of North Carolina

# Who is TSE Services



- TSE Services is an independent, customer-focused company providing easy and affordable access to information and communication solutions
- Provide competitive information technology and telecommunications services to NCEMC, EMCs, and other entities to allow those organizations to focus on their core businesses and competitive challenges

# What is SEIM

- Security Event Information Management
- Technology used to analyze security event data in real time for internal and external threat management, and used to collect, store, analyze and report on log data for regulatory compliance and forensics
- Also known as SIEM

# Two Main Functions

- SEM
  - Processes log and event data from security devices, network devices, systems and applications in real time to provide monitoring, correlation, and incident response
- SIM
  - The collection, reporting and analysis of log data to support regulatory compliance reporting, internal threat management and resource monitoring



# SEIM Requirements

- Must be fast
- Multiple parsers
- Achieving and retrieval
- Clear concise reports
- Filter noise



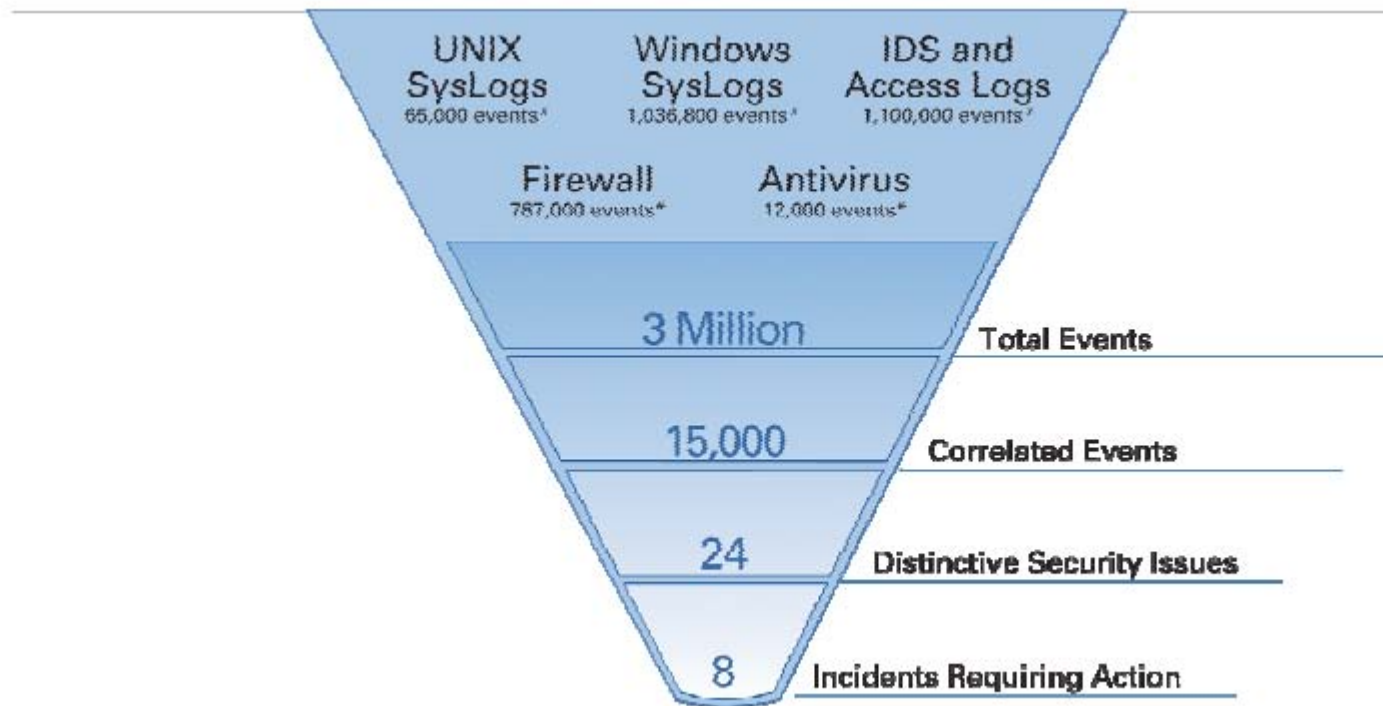


# Business Drivers

- Risk is higher than ever
  - Network attacks have doubled (Deloitte Global Survey)
  - 70% of security incidents involve insiders (Gartner)
- Accountability
  - Need to reduce corporate risk
  - Need to demonstrate regulatory compliance
- What we don't know is costing us
  - Security incidents costs corporations over \$21 million per incident (Forrester research)
  - Over 30% of corporations don't know how many security incidents they have (FBI cyber study)



# There is not enough time



# How do you show compliance

- PCI requires that you log when a users privilege has been escalated to root or administrator level
- You must log all router and switch configuration changes
- Security incidents must be detected, logged, and forensics must be performed
- Reports and logs must be available during an audit



# Vendors

- CoreTrace
- ArcSight
- Cisco
- ISM
- LogLogic
- NetIQ
- Q1
- RSA
- Computer Associates

# Wrap up

- Happy to take questions
  - See me after the meeting or tonight

